

CLAIMS

1. A monitor that monitors the security state of a remote computer system, the monitor comprising:

5 a computing device;

a communications medium interconnecting the computing device with the remote computer system;

a pair of data-storage media each containing a sequence of encryption keys, one data-storage medium local to the monitor, and the other data-storage medium local to the remote computer system; and

10 a program, running on the computing device, that exchanges with the remote computer system, over the communications medium, messages encrypted using one or more encryption keys extracted from the data-storage medium local to the computer system in order to monitor the security state of the computer system.

15

2. The monitor of claim 1 wherein, following power on or reset of the computer system, while the computer system is in a relatively high-security state, the computer system sends an initial-authentication message to the monitor, encrypted with a next key extracted from the data-storage medium local to the computer system.

20

3. The monitor of claim 2 wherein the monitor receives the initial-authentication message, decrypts the initial-authentication message using a next key extracted from the data-storage medium local to the monitor, and stores an indication that the computer system is in a relatively high-security state.

25

4. The monitor of claim 2 wherein the computer collects security metrics and includes the security metrics in the initial-authentication message.

5. The monitor of claim 4 wherein the monitor receives the initial-authentication message and extracts the security metrics in order to determine the security state of the computer system.

30

6. The monitor of claim 1 wherein, while the computer system is in a relatively high-security state, prior to loading and/or executing an untrusted software program into memory, the computer system sends a going-insecure message to the monitor, encrypted
5 with a current key extracted from the data-storage medium local to the computer system.

7. The monitor of claim 1 wherein the monitor receives the going-insecure message, decrypts the initial-authentication message using a current key extracted from the data-storage medium local to the monitor, and stores an indication that the computer
10 system is in a relatively low-security state.

8. The monitor of claim 1 wherein the data-storage media both contain identical sequences of encryption keys, and each of the data-storage media are one of:
a compact disc;
15 a DVD disc;
an electronic memory; and
a magnetic disk.

9. A method for monitoring and reporting the security state of a remote
20 computer system, the method comprising:
providing a monitor computing device interconnected with the remote computer system by a communications medium;
providing a pair of data-storage media, each containing a sequence of encryption keys, one data-storage medium local to the monitor computing device, and the
25 other data-storage medium local to the remote computer system; and
receiving messages from the remote computer system over the communications medium by the monitor and storing an indication, by the monitor, of the security state of the computer system determined by the monitor from the received messages.

30 10. The method of claim 9 further including receiving, by the monitor, a request for information about the security state of the computer system, and replying with a

security-status-inquiry-response message by the monitor based on a determined security state of the computer system.

11. The method of claim 9 further including, following power on or reset
5 of the computer system, while the computer system is in a relatively high-security state, sending, by the computer system, an initial-authentication message to the monitor, encrypted with a next key extracted from the data-storage medium local to the computer system.

12. The method of claim 11 further including receiving, by the monitor, the
10 initial-authentication message, decrypting the initial-authentication message using a next key extracted from the data-storage medium local to the monitor, and storing an indication that the computer system is in a relatively high-security state.

13. The method of claim 11 further including collecting, by the computer
15 system, security metrics and including the security metrics in the initial-authentication message.

14. The method of claim 13 further including receiving, by the monitor, the
20 initial-authentication message and extracting the security metrics in order to determine the security state of the computer system.

15. The method of claim 9 further including sending, by the computer
system, a going-insecure message to the monitor, encrypted with a current key extracted from the data-storage medium local to the computer system, while the computer system is in a
25 relatively high-security state, prior to loading and/or executing an untrusted software program into memory.

16. The method of claim 15 further including receiving, by the monitor, the
going-insecure message, decrypting the going-insecure message using a current key extracted
30 from the data-storage medium local to the monitor, and storing an indication that the computer system is in a relatively low-security state.

17. Computer instructions implementing the method of claim 9 encoded in a computer-readable medium.

5 18. A monitor that monitors the security state of a computer system by the method of claim 9.